

THE COLLISION OF INTELLIGENCE AND INFORMATION

Robert D. Steele-Vivas, MA MPA NWC
President, OPEN SOURCE SOLUTIONS, Inc.

Suddenly, confounded by the disappearance of the monolithic Soviet threat, which has justified multi-billion dollar intelligence budgets since the National Security Act of 1947 created the Central Intelligence Agency and related capabilities, the intelligence community has rediscovered unclassified public information, or, in its jargon, "open source intelligence" or OSCINT.

Now, confronted with the proliferation of issues and targets which it is not prepared to monitor, the intelligence community has realized that OSCINT is frequently the only source available; and at the same time begun to recognize that unclassified public information is a very cost-effective way of meeting policy-maker needs while contributing to national competitiveness.

The appointment of an Open Source Coordinator by the Director of Central Intelligence, responding to Congressional pressure, has set the stage for a collision between the worlds of "black" intelligence, and "white" information. The coming year is certain to see intense debate about the missions, role, and structure of the intelligence community; and about how the government should manage its participation (and/or competition) in the world of unclassified data acquisition and production.

There are four major areas of inquiry likely to receive attention in the future:

first, whether the intelligence community should be competing with private sector providers of unclassified analysis and products;

second, whether the intelligence community should disseminate unclassified intelligence products into the public domain;

third, whether the intelligence community should release into the public domain information about its multi-media collection and processing technologies; and

fourth, whether a significant portion of the intelligence community's

budget--on the order of \$1 billion a year-- could be used to fund a dramatically increased National Public Network (NPN), one which extends the National Research & Education Network (NREN) to every home and office while also radically increasing joint government-private sector efforts to collect multimedia data on behalf of the broader electronic public.

Coinciding with the intelligence community's discovery of the utility of unclassified information are changed perspectives within the business world, where managers are finding that "competitive intelligence" is not only essential to their survival, but that they must also monitor demographic and economic trends, environmental costs, and many other complex issues which bear on profit margins. Despite some "red herrings" (see the review of FRIENDLY SPIES at the conclusion of this issue), most enterprises seem to understand--as Alvin Toffler and others have articulated--that information is a corporation's most important asset, and that every enterprise needs a (predominantly unclassified) intelligence collection and processing campaign plan.

Unfortunately, despite a vast range of multimedia and multi-lingual sources of information, and a proliferation of information handling technologies and government/private sector contracts for coping with information overload, there is as yet no useful national architecture or strategic plan for improving access to unclassified information for government employees, business analysts, or individual citizens and students. The entry of the intelligence community, and its budget, into the public information arena will challenge the leadership abilities of the Administration, and could be the basis for substantive political and economic debate by all information industry associations and enterprises.

The Vice President and his staff, could if they choose to do so, make a difference and contribute to national competitiveness by ensuring the inclusion of the intelligence community in our national "information continuum" which runs "from school house to White House". Among the essential initiatives the Vice President must consider: that of a public intelligence agency, one responsive to the needs of individual citizens, voters, and shareholders, and one untainted and unencumbered by the dead weight of security restrictions and perspectives developed during the Cold War. As John Perry Barlow has stated so well, "the secrecy paradigm has lost, the openness paradigm has won". Let us get on with the reengineering of the U.S. intelligence community, and focus on objectives and outcomes, rather than sources and methods.

Intelligence Community Seeks New Security Structure Role

By Col. Alan D. Campen,
USAF (Ret.)

The demise of Iron Curtain targets and the alleged irrelevance of things once garnered surreptitiously by spies, satellites and other devious black arts have led Congress and many new experts in the intelligence domain to call for starkly different collection, analysis and dissemination techniques.

In its quest for *raison d'être*, the intelligence community confronts an alien paradigm in which business and the public, not the president, are the principal clients; where economic competitiveness, not massed armies, is the major threat; and where the principal source of intelligence lies not in the minds and safes of foreign leaders, but is available in the public domain, some experts believe.

Intelligence community leaders are scrambling to define and claim a role for their national foreign intelligence apparatus within a new national security structure. As they face the threat of huge budget cuts, the leaders say they also must sort through profuse but conflicting advice on the requirements of a changing mission.

Those who urge a different course for national intelligence proffer disparate views on the disposition of the Cold War intelligence structure, industry experts report. U.S. national security has been redefined, the experts explain, to include industrial competitiveness, regional conflicts, nuclear terrorism and environmental protection. The intelligence community now must prove that Cold War organizations, methods and tools are relevant to the challenges of an uncertain, volatile and multipolar world.

New Threats, New Tools

U.S. national security rests on two pillars—economic stability and military strength, but the economic element is in clear and present danger, the experts warn. Former Marine Corps intelligence executive Robert David Steele contends that national

security can no longer safely be founded solely on military supremacy. Our security includes the “preservation of our national culture, of our way of life [and] of the conditions which permit the pursuit of happiness and prosperity,” he avers. Steele, who now is associated with Open Source Solutions, Falls Church, Virginia, explains that the present intelligence structure must be altered because it is not up to such an expansive tasking.

The Clinton administration’s Economic Security Council inevitably will press the Central Intelligence Agency and the National Security Agency for intelligence that may be of a different character than previous requirements, the experts indicate. Nevertheless, this intelligence will

Intelligence approach calls for fewer secrets, open sources, dissemination and outsourcing.

be no less urgent than current National Security Council needs, they add.

Open source is a new shibboleth for the ancient art of listening. However, where merchants once sent spies into the markets to probe for the pulse of trade, today the secrets thought so vital to economic survival freely flow through the airwaves. They are fair targets for anyone inclined and equipped to eavesdrop.

Market Approach

Open source intelligence now is enshrined as a co-equal to human and signals intelligence, the experts say. Data that once were confined to corporate board rooms or the eyes of only the most senior executives now routinely reside in desktop computers. These machines are interconnected by unprotected and vulnerable local and wide area communications networks, the experts warn.

Herbert E. Meyer, former special assistant to the director of Central

Intelligence and now engaged in the business of intelligence, argues that the leading edge in economic warfare comes more from “vision than from raw strength.” According to Meyer, information systems are the defining technology of this new age. He indicates this is because correlation software technology enables industry to reach into and pull from the torrent of vital information flowing in the ether those data upon which the fate of enterprise turns.

Advocates of open source intelligence assert that all but the world’s most critical secrets can be retrieved or reconstructed from the information that routinely flows over global computer networks. A Republican task force in the House of Representatives claims to have employed open sources to forecast both the Iraqi invasion of Kuwait and the transfer of nuclear weapons from Islamic republics in the former Soviet Union to Iran.

Author John Petersen agrees, writing that “the government’s fixation on tightly controlled classified information, for example, was a major contributor to their completely missing the collapse of the Soviet Union, indications of which were freely available in open, unclassified literature.” His paper, “Staying in the National Security Business: New Roles for the U.S. Military,” was included in the proceedings of the recent National Competitiveness: Open Sources Solutions Symposium.

Meyer says that intelligence is at the “heart of an information gathering and monitoring process whose value to policy makers will be even greater in the less dangerous—but vastly more complex—post-Cold War world” and that “intelligence isn’t spying...[but] the hot new management tool for competing—and winning—in today’s business world.”

The controversy that churns within this open source theorem involves the role of the Central Intelligence Agency in economic warfare and how government intelligence activities would interact with a highly competitive U.S. industry. The essence of this controversy was aired

by Michelle Van Cleave, who was assistant director for national security affairs and general counsel, Office of Science and Technology Policy, Executive Office of the President, in her article "World Economic Rivalry Poses Policy Changes," (*SIGNAL*, May 1991, page 74).

Meyer thinks the national intelligence apparatus, principally the Central Intelligence Agency, holds the lead in correlation technology. Of even greater significance, according to Meyer, it holds those talents, disciplines and analysis methodologies required to turn raw data into timely information and then into useful intelligence for clients, be they warriors or economists.

Budget Cuts

A vocal minority at the margin in this continuing debate argues that the Cold Warriors are anachronisms, with no place in the new scheme of things; that the threat has shifted to regional conflicts and to terrorism; and that the old tools of the trade must give way to emphasis on human intelligence.

Crowing that the much vaunted sensors in space could count Soviet

strategic missiles but not perceive the impending implosion of an economic and political structure, they argue for a sharply reduced Central Intelligence Agency role in the newly defined national security environment. And they clamor for large cuts to the national foreign intelligence budget.

While the Bush administration and Congress did cut tactical intelligence by 25 percent, the national foreign

*The value of
intelligence drops
dramatically
with each increase
in level of
classification*

intelligence program (NFIP) is reported by *The Washington Post* to hover still around \$17 billion, or near its Reagan administration highs.

Many Democratic lawmakers believe that, in light of the collapse of communism and the need for cost-cutting, intelligence agencies' bud-

gets should shrink as well. The Clinton administration, however, appears to be responding to the warnings associated with deep reductions in the intelligence budget. The administration has put in motion efforts to protect the nation's \$29 billion intelligence budget from immediate cuts, according to a recent *New York Times* service column.

Robert Gates, former chief of the Central Intelligence Agency and director of central intelligence, responds that the changes in threat are clear signals to maintain a strong national foreign intelligence program, not for massive cuts. Further, he asserts, the notion of open source collection and analysis is nothing new, having represented a major, if unheralded, portion of the Central Intelligence Agency's work for years.

Other advocates of a new approach to intelligence deprecate the traditional, covert searching for secrets and the resultant imperative to protect sources and methods. Steele believes that the value of intelligence "drops dramatically with each increase in level of classification" and has written that "secrets are

Mark Your Calendar Now!

April 13-14, 1994

Ottawa Congress Centre



AFCEA Canada '94

Global Operations: Responding to Change

Invitation to Exhibit— *Exhibit fees are being held at 1992 levels!*

If your company provides equipment or services to the Canadian Government's Information Technology Community, you are cordially invited to exhibit at AFCEA Canada '94. This show is sponsored by the Ottawa Chapter of AFCEA for the Canadian AFCEA region. Reserve your space at AFCEA Canada '94 now by contacting Marion G. Fuller, Conference Manager, AFCEA Ottawa Chapter, at (613) 594-8788.

Call for Papers

Papers are invited that pertain to the theme *Global Operations: Responding to Change*. Possible subjects of interest are integrating technologies for global operations, technology diversification in a changing world, equipping a professional peacekeeping force for today's global operations or the expanding C⁴I requirements for global operations—an operator's view. All papers must be unclassified. Authors must obtain company and/or military clearance prior to the final submission of papers. Send abstracts to the Program Chairman, AFCEA Canada '94, 201-251 Laurier Ave. W., Ottawa, ON., Canada K1P 5J6.

Author Schedule

Deadline for summary: **September 30, 1993**

Acceptance Notification: **November 30, 1993**

Full copies of presentation and author details (photos, etc.): **January 28, 1994**

inherently pathological, undermining reasoned judgment and open discussion." The true value of intelligence to the nation, Steele says, "lies in its informative value, a value which increases with dissemination."

Under the approach that Steele advocates, intelligence—once highly classified and privy to a select few at the top—would be widely and freely shared with a multitude of decision makers within and outside of the government. * →

Nuclear Armed Terrorists

Still other experts argue that our national foreign intelligence structure has more pressing matters at hand in the neo-nuclear world than servicing the competitive drives of U.S. industry. They decry that tactical nuclear missiles are within the grasp of zealots and other non-deterables and that the role of national intelligence should be refocused on new military threats rather than being expanded to include economic warfare.

The changes proposed by these experts would give far greater emphasis to human intelligence, to language skills and to a greater understanding of indigenous Third World cultures and problems. They foresee from this an intelligence process more tuned to the intent of enemies rather than their capability. Intelligence products in this structure would help decision makers become more proactive and assist them in predicting future incursions, such as the Iraqi invasion into Kuwait.

When speaking in defense of the current NFIP budget, former director Gates has argued that just such a shift in analytical emphasis already had taken place within the Central Intelligence Agency and that "fewer than 15 percent of the resources are going to the former Soviet Union." Many experts agree with Gates, pointing out that the agency holds trump on analysis skills and methods and can and must lead the modernization effort.

Perhaps, but not enough, says Steele, who argues that "human insight is the essence of intelligence," and this human factor cannot be replaced by any amount of automation. Analysts today are "cloistered away from their customers, the policy makers and the action officers and have little significant interaction with their academic, industrial and foreign counterparts," Steele contends. Government analysts need more time for travel,

reflection and interaction with private-sector analysts, he warns.

Outsourcing Intelligence

Social pundit Alvin Toffler probably would hold moot these disputes over the role of the Central Intelligence Agency in economic intelligence. In *Power Shift*, he writes "we are about to see a fusion of government and private business intelligence on a scale never before known"; that the "link between public and private espionage will continue to blur"; and that organizations such as the Central Intelligence Agency will contract out more work. This, he suggests, is because "they cannot recruit, maintain and pay for all the necessary specialists" to meet demands from government policy makers for information on economics, technology and the environment.

Toffler says the basis for outsourcing intelligence already is being laid by the proliferation of private research "boutiques" specializing in everything from political risk analysis to technical information searches. The privatization of intelligence capabilities, including overhead imagery and signals collection, processing and dissemination, significantly will influence the nature of government-sponsored intelligence activities, he contends.

New Rules of Engagement

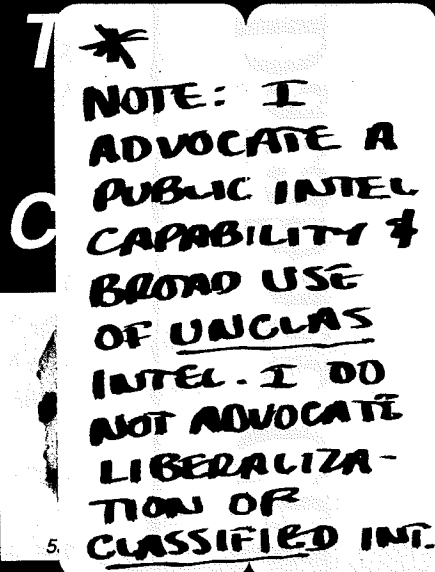
While the new theology of information holds that intelligence is as vital to economic warfare as it is to military superiority, economic espionage is, nonetheless, an unfamiliar form of warfare to the government. Gathering this type of information posits radically different rules of engagement from the methods that served the intelligence community so well in its struggles against the Soviet Union, the experts say.

Widespread agreement among these experts exists that national security remains founded on sound intelligence—whether the threat be regional nuclear, terrorism, drugs or economic supremacy. However, the experts have not reached a consensus on how, or even if, the Cold War trappings of the intelligence process fit into the kit bag for waging economic or regional warfare.

• • • — • • •

Col. Alan D. Campen, USAF (Ret.), is manager of AFCEA International Press and is a member of the AFCEA Northern Virginia Chapter.

Finally, a BERT



• Performs

- Full Bit Error Rate Testing
- Event timing and remote testing
- Tests from 50bps to 13Mbps

• Electromagnetic Interference Compliance (EMI)

- Complies with MIL-STD-461C and MIL-STD-462 as specified in MIL-T-28800

• Interface Options

- A full range of plug-in modules that permit testing of U.S. and European standards including MIL-STD-188-114

• Selected by the U.S. Navy as the G.P.E.T.E Bit Error Test Set



PHOENIX

991 Discovery Drive
Huntsville, Alabama 35806
205-922-1200 / 800-866-8480

Test Smart... Test Phoenix

Circle 112 on Reader Service Card

DoD Database Colloquium '93

Evolving Standards for Joint Interoperability

August 22-25, 1993

San Diego Princess Hotel
San Diego, California

Sponsored by: The DoD Database Colloquium Coordinating Committee

In Cooperation with:

The DoD Center for Information Management (CIM)
The Naval Command and Control and Ocean Surveillance Center
The Naval Computer and Telecommunications Command
and the Naval Security Group Command

In Coordination with and Administered by: AFCEA

This is a banner year for the Database Colloquium, marking its 10th Anniversary – a decade of service to the information management community. And, in celebration of the importance of this event, we proudly announce that the DoD Center for Information Management (CIM) has joined the Colloquium team.

The major goals of the Colloquium are to exchange information on information resources management problems and present requirements and proposed solutions, provide discussions on the broad range of applicable technologies, provide policy guidance applicable to DoD and civil agency information resources managers, and identify and encourage service-unique and government-wide standardization efforts and information/technology transfer.

Program, Registration and Exhibit Information:

Programs Office
AFCEA International Headquarters
Tel: (703) 631-6125 / (800) 336-4583, ext. 6125
Fax: (703) 631-6133

SIGNAL Advertising Information:

Tel: (703) 631-6181 / (800) 336-4583, ext. 6181
Fax: (703) 222-8762

It is our sincere desire to comply fully with both the letter and spirit of the Americans with Disabilities Act of 1990. Attendees with special needs should call (703) 631-6125 so we can ensure that your visit at our Conference is a pleasurable one.

National Security and National Competitiveness

by Robert D. Steele

With the creation of the National Research and Education Network (NREN) and its sponsorship by (now-Vice President) Al Gore, the intelligence community must now define and enhance its role within the overall information environment of the nation. Through [Vice President] Al Gore's initiative, the intelligence community and the information industry have the opportunity to alter radically the way we do business, not only within the American information environment, but also, by extension, the international information environment. The NREN initiative represents one of those rare catalytic events which can change our lives.

Imagine an extended network of citizen analysts, competitive intelligence analysts in the private sector and government intelligence analysts, each able to access one another, share unclassified files, rapidly establish bulletin boards on topics of mutual interest and quickly pull together opinions, insights and multimedia data which is all the more valuable for being immediately available without restrictions.

That is where we need to focus by looking at what the intelligence community needs to do in the open source (i.e., unclassified) arena and at how the intelligence community and the information industry might better support the rest of government and the private sector to improve national competitiveness. A few points can be highlighted.

On consumer needs. The military consumer in particular, but all government consumers as a rule, have made their needs clear: they want unclassified information that is timely, "good enough" and easy to share (i.e., without classification restrictions).

During a recent two-year stint as the civilian special assistant to the director and deputy director at the new USMC Intelligence Center at Quantico, attempting to meet Marine Corps needs for basic encyclopedic intelligence about the Third World, including such details as bridge loading and tunnel clearance, I learned two things: much of what we need is not in the national (classified) databases because of our recent preoccupation with the Soviet Union; and much of what we need is available from private sector sources.

This experience, reinforced by my participation in Technology Initiatives Game 1992, an effort to test information handling concepts, persuaded me that expeditionary/littoral operations, and particularly those dealing with humanitarian assistance missions to the Third World, could be relatively well served through the collection, processing, analysis and dissemination of unclassified, or open source, information.

Regarding data changes. Both positive and negative trends are evident in the area of data changes. On the positive side, vastly more data is available for digitalization, and multimedia is electronically available. On the negative side, data management methods

are antiquated, and no commitment to this area is being shown by government or the private sector. A national knowledge architecture, with international exchange agreements in all areas, is as urgent a national priority as strategic nuclear deterrence once was.

But again on the positive side, the new administration appears to be focusing on these issues as a matter of course. Many of us have been asked to share our thinking with administration officials through direct discourse, as well as through electronic calls for input.

Major changes are occurring in software, specifically software able to convert and fuse multimedia data. "Smart" software is coming along more slowly, in part because we have not been aggressive about debriefing experts and developing heuristics. We need to do much more in the area of knowledge-base building, even if it means, as some have done so effectively in the signals environment, that we must capture hundreds of work years of heuristics against the day when we can quickly convert these heuristics into exploitable software.

Organizational changes. The biggest organizational change is the trend toward privatization of intelligence and the availability of virtually any information desired from a private sector source. That is especially helpful now, as we attempt to transition from an intelligence community focused narrowly on a single major con-

ventional threat, to one able to deal with a wide variety of non-traditional emerging threats. Former Commandant of the Marine Corps, General Alfred M. Gray, provides an enlightened distinction between conventional and emerging threats.

The conventional threat has generally been associated with a specific government; consisted of conventional and nuclear tools with relatively static orders of battle; developed new capabilities in linear fashion, moving from research to operational testing to fielding; accepted clear rules of engagement; followed a known doctrine; provided ample strategic warning; and been supported by relatively well-marked intelligence assets.

The emerging threat, by contrast, is generally non-governmental; non-conventional in nature; dynamic or random in its emergence, lifespan and actions; and non-linear in development of its capabilities, buying or stealing what it needs. The emerging threat accepts no "conventions" or rules of engagement; has no known doctrine; is almost impossible to detect in time for warning of attack; and has an unlimited fifth column in the form of criminals, druggies and plain scared citizens that will provide one-time support in extremis.

In the face of such challenges, it is our task to integrate the strengths of the intelligence community with those of the information industry and to develop specific strategic and operational plans for executing open source collection, processing, analysis and dissemination initiatives in fiscal years 1994 and beyond. We cannot succeed in this effort if we do not broaden the consumer base for intelligence community products.

In particular, we must rethink the role of the intelligence community in supporting the non-defense sectors of government and the private sector, usually with increased emphasis on open source collection and unclassified intelligence production.

I do not believe that we should be in the business of providing classified information to the private sector, even when we discover cases of foreign government subsidies or joint foreign government-private sector industrial espionage against American enterprises. The world is too international

and ownership of enterprises too cloudy to permit those judgments to be made with any consistency or justice.

But I do believe that the United States and other nations desperately require increased government investment in information technology and in the collection, processing, analysis and dissemination of unclassified multimedia, multilingual information. For too many years I have seen enormous waste in our collection of open sources, both in terms of what we capture and spill and in terms of the vast quantities we do not capture, and also enormous waste as each of our separate intelligence programs has attempted to develop the ultimate all-source workstation. This must stop.

The NREN initiative is a superb starting point from which to consider the establishment of an intelligence community network for receiving and disseminating unclassified information. The intelligence community has an obligation to support NREN by participating in an expanded version of this national information infrastructure.

Our challenge is to establish standards, generic requirements and free exchanges of information, not only between the U.S. government and its private sector, but also among different U.S. government agencies, U.S. government and foreign governments, and U.S. and foreign enterprises and institutions. Every serious student of intelligence, and the leaders of the intelligence community, accept the fact that intelligence pipelines are no longer affordable and are, in fact, counterproductive to the creation of fused all-source intelligence. Unclassified information and unrestricted networks must become the "source of first resort" within the intelligence community and the foundation for value-added fusion of classified imagery, signals and clandestine human intelligence.

For those concerned about the value and security of information and the merits of concealing information for competitive advantage, we must remember that the value of information is insured through handling more and more information quickly and effectively, not through attempting to hoard selected information.

The kind of protection previously provided by highly technical and

highly focused systems dedicated to a single, known threat is now available only through the broadest possible sensor string, one that takes in multimedia, multilingual information and disseminates it to the right person in the right format at the right time. Only open source information is cheap, flexible and readily exchangeable among allies and private sector partners, and offers enormous returns on investment, both in terms of national security and in terms of national competitiveness.

Information, as a substitute for violence, capital, labor, time and space, offers us the opportunity to be competitive in the future. And being competitive through smart information policy can mean the achievement of prosperity without conflict.

This opportunity provides areas for significant contribution by the private sector. First, the worldwide data entry problem is clearly beyond the government's ability. While the foreign broadcast information service has worked hard to meet needs in this area, government cannot cover all the bases. The market for raw multimedia, multilingual data exists and the private sector needs to accept this challenge.

In addition, we have been remiss in failing to put time and space tags on data as it is collected. We need to develop more sophisticated means of labeling data in relation to the specific time and geographic location associated with its content and its genealogy. Data today generally does not have an understandable, i.e., machine-readable, time and space context. That's something to think about.

Classification of information and attempts to restrict its dissemination are inherently counterproductive because they slow the feedback loop to the point that the classified information is relatively useless in comparison to open source information that is timely and immediately available. The pendulum has swung. Our warfighters, including our economic warriors, have made clear that classified intelligence with all of its handling constraints is too slow and too late. Unclassified information, while not perfect, is good enough—and in many instances better than classified intelligence because of its timeliness, its flexibility and its availability.

U.S. Intelligence: Coming Out of the Cold Into the Information Age?

by Lois F. Lunin

Question: What do James Bond (007) and a CIA analyst have in common? Answer: The search for strategic information.

While James Bond has operated in the field, for the most part the U.S. intelligence community has worked in offices using classified information. With the Cold War collapse and global political

changes, the intelligence community is restructuring and shifting to increased use of open sources.

To begin a dialog between the information and intelligence communities, Open Source Solutions, Inc. (OSS) held its First International Symposium December 1-3 at Tyson's Corner, VA. The symposium focused on National Security and National Competitiveness: Open Source Solutions.

Obsession with Secrecy

Intelligence is facing decreasing resources and, at the same time, dramatic increases in the complexity of the international environment and technologies. Because classified capabilities had focused almost exclusively on the Soviet Union, the U.S. is now relatively unprepared to monitor and understand

non-traditional Third World threats including those to the environment, explained Robert D. Steele, OSS president.

Today definitions are changing in technology, intelligence, security, and national competitiveness. There are nearly 18 million PCs in the U.S. today, more than in the rest of the world combined, said George A. Keyworth, II, Distinguished Fellow, Hudson Institute. We live in a "distributed information economy." Classification is a handicap and too hard to protect. Yet a gap exists between intelligence adapting to the information age and the population as a whole. Government should go from an obsession with limited to distributed information and become an enlightened customer. Unclassified or open source (OS) information has been shown to be a substitute for and a complement to more expensive, or unavailable, classified intelligence.

Open sources include the domestic and foreign press, associations, academia, government agencies, databases and bulletin boards, and personal interviews, Lt. Gen. James Williams, (USA Ret.) explained.

Turning to Open Sources

Intelligence people are information hounds, explained Admiral William Studeman, Deputy Director, CIA. Intelligence and media are in the same business. The goal is to glean information from other sources. Sometimes public information is the only information about events and crises. And, Studeman added, open sources should be the first step in gathering information.

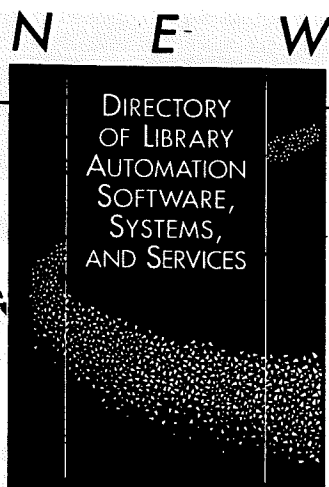
Speakers warned, however, that open source information can be biased and misleading. It requires strong information analysis, for example, comparing current content with past action. Yet sometimes open source information is more accurate than classified.

Today most open sources are extremely valuable to intelligence, even more so now that there are a greater number of sources worldwide. About 8,000 commercial databases are of some intelligence value; some 1,700 newspapers were not published a year ago.

Television is a relatively new area for intelligence activity and provides a look at a country's activities that neither the OS literature nor the news offers. Covered 790 hours a week in 29 languages, TV gives a broader knowledge of restricted areas.

"Open systems means you can do things without the permission of the bureaucracy: a critical point in a high-change world," declared John Gage, Director, Science Office, Sun Microsystems Laboratory. How do you approach the future? Open systems are the key to staying close to the curve. "We are creating ways of seeing and understanding that have not been possible in the past, and that allow actions we could not imagine before." Wireless connections: satellite (low orbit, lower power), spread spectrum, infrared, light modulation, and more.

(continued on next page)



Directory of Library Automation Software, Systems, and Services

Edited by Pamela Cibbarelli

Published biannually since 1983, the **Directory of Information Management Software for Libraries, Information Centers, Record Centers**, retitled the **Directory of Library Automation Software, Systems, and Services**, is recognized as the primary reference source for software packages used in automating libraries.

This entirely new expanded 1993 edition provides detailed descriptions of about 250 currently available microcomputer, minicomputer, and mainframe software packages and services. The 1993 edition contains more comparative information on library applications software than is available from any other source.

Analysis for each software package includes the following:

- Hardware/Systems Requirements
- Applications
- Updating/Reporting Modes
- Search Logic
- Record Structures
- Availability
- Documentation
- Training
- Installation Sites
- Costs
- Name of Vendors
- Comments by Vendors and Who to Contact for Additional Information
- All packages are indexed by product name, computer hardware, vendor, and type of application

The directory also includes:

- Information Management Software
- Full Text Retrieval Software
- A Selective Bibliography for Library Automation Books and Serials on Software Packages Published Since 1990
- CD-ROM Distributors
- Records Management and Library Automation Consultants

- Retrospective Conversion Products and Services
- About Fifty Recurring Conferences and Meetings
- Hosts of Library and Information Science Databases
- Citation Management Software.

Order Your Copy Today!

1992/350pp/softbound/ISBN: 0-938734-65-2

Price: \$79.00

Express Order Service: Call 609/654-6266

24 Hour Fax Order Service: Call 609/654-4309

Mail Orders: Complete & Mail The Form Below

Learned Information, Inc.

143 Old Marlton Pike, Medford, NJ 08055

Please enter my order for _____ copies of the 1993 **Directory of Library Automation Software, Systems, and Services** at \$79.00 each, and add \$3.50 shipping and handling for the first book and \$3.00 for each additional book:

Name _____

Title _____

Organization _____

Address _____

City _____

State/Zip _____

Daytime Phone _____

Method of Payment

☐ Bill me PO # _____

☐ Payment enclosed

Charge to my:

☐ MasterCard ☐ Visa Exp. Date _____

Account # _____

Signature _____

U. S. Intelligence

(continued from previous page)

Challenges to the Intelligence Community

The biggest challenge to the intelligence community is the processing of vast amounts of data, filtering, storing, and manipulating it. Intelligence probably processes more information than any other organization in the world. At the highest level information from all sources is fused and analyzed.

Another challenge: One agency does not necessarily know what another has. There is no capability to share electronic information. Steps are being taken to catalog OS so that the data can be shared. CIA director Robert M. Gates recently appointed an OS coordinator; this should provide a focal point for developing a program together with the private sector.

Today business intelligence systems are several light years ahead of government, said Herbert Meyer, Chairman, Real World Intelligence, Inc., and former vice-chairman, National Intelligence Council. Industry has not been hobbled by bureaucratic classification and the Cold War.

Part of the problem, as observed by several speakers, seems to be technological, with analysts lacking tools for information seeking. Part is organizational with management unwilling to let its officers out to talk with counterparts in other agencies and preventing the development of OS collection, processing, and dissemination capabilities.

Issues, Impediments, Problems

"Use of open sources present several potential problem areas including imprecise requirements, failure to understand the sources, inadequate search algorithms, overwhelming volume, gaps in holdings, and lack of analytic experience," Williams noted.

Other information problem areas include a lack of a national information policy, preoccupation with short term vs. long term growth, legislatively-caused problems, and lowest bidder contracting, explained Marjorie Hlava, president, Access Innovations.

New issues of concern to both government and the private sector, as identified by Kenneth Allen, president, Information Industry Association, are privacy, pricing of subscriptions, cultural identity, and shifting ways of customers.

One impediment he pointed out between government and industry is a difference in attitude and politics. Another is how government describes its mission: The language is confusing. Allen cited as one example the use of the word *exploitation* of sources, a sensitive word to industry. A third impediment is the perception—mistaken—that government speaks with one voice, that one agency speaks for all.

Still another red flag he cited is the interpretation of intellectual property by some agencies. Where the government indicates that the intellectual property right must not be tolerated, the information community considers this a basic right. [Is

this a semantic or an actual problem?]

Allen emphasized that the guaranteed right to public access and production of information is what sets us apart from the rest of the world. In every other country, he stated, government owns the information. The challenge he sees: Government and the private sector must work together but not shake the principles we've lived by for more than 200 years.

We oversell concepts and ideas and technology, said Dr. Stephen Andriole, Drexel University, and overlook marrying technology to problems. The under exploitation of information technology includes long neglect of analysis vs. collection; shortage of analytical process modeling; limited application of com-

puter-based analytic methods; suboptimal staffing and training; and the cult of the "artist" vs. the "engineer."

Who Are Our Enemies Now?

One of our enemies is fraud and another the sheer volume of overwhelming information that can defeat us in war, explained Robert Hutchinson, Jane's Information Group. Open sources give a good first pass. They offer the convenience of having the bulk of information in one place and provide for free discussion—but OS is not a panacea for intelligence communication. Much of the huge volume of information, he noted, is rubbish, plagiarized, and reproduced in a different form.

Some serious matters must be dealt with in the information itself, stated John Perry Barlow, Electronic Frontier Foundation (EFF). Is it meaningful? Intelligence people are good at determining this. There is lots of noise and an incredible din and it's important to figure out that which is relevant and pertinent.

Protection of Intellectual Property

The Age of Cyberspace presents other new problems in handling OS information: The lack of conventions in how to deal with information and major accounting problems in how to track the use of specific information, explained Brian Kahin, Harvard University. Electronic
(continued on next page)

Enhance your access with our complements!

New!... Microcomputer Index on magnetic tape

Looking for information on computer use in business, education, and the home? There's no better source than Learned Information's Microcomputer Index. And one of the best ways to access it is through the Database Licensing Program at UMI.

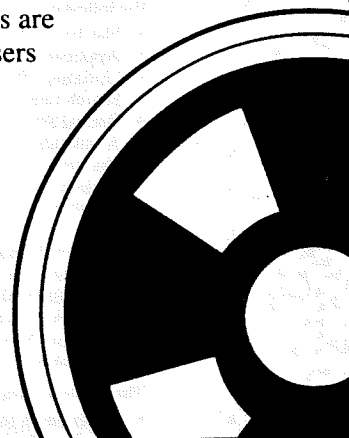
THE DATABASE: Microcomputer Index, published by Learned Information, is the perfect complement to your library's holdings. It's an indispensable guide to the world of computers. It offers abstracts and indexing for articles from seventy-five top computer periodicals, including *BYTE*, *Compute!*, *Mac User*, and *PC/Computing*. You get more than 50,000 citations to articles (1989+) on a wide range of computer-related topics. Your users are guaranteed to find the information they need.

THE PROGRAM: UMI's Database Licensing program offers curricula support, easy search and retrieval using your own automation software, full-text support, unlimited local access, and limited, predictable costs. The price is determined by the number of locations and simultaneous users, not by the amount of time spent on the system or the number of searches performed. Licensing database from UMI is easy and cost-effective. And since the databases are mounted on your library's own system, your users don't have to learn new search routines.

Microcomputer Index on magnetic tape offers all the computer information your users need, easily accessible on your own system. You'll be showered with compliments!

To find out how, just call
toll-free 800/626-2823, ext. 226.

U·M·I



U. S. Intelligence

(continued from previous page)

form makes it very easy to take and republish proprietary information.

There is a lack of control by rights holders, a need for authentication of information, and warranties—citations, best efforts protection and preservation, and errors and omissions exemption, said Robert Kahn, president, Corporation for National Research Initiatives (CNRI).

Information producers have a need to control access, identify response, and maintain data integrity, while consumers have a need to protect their interest and their intent. Technology permits highly

assured user ID; control over user access to data; resistance to external attacks; and the ability to protect data from storage to reader, predicts James Anderson, a computer security expert.

Significant challenges yet to be met for the military include widely available OS literature; production and dissemination which must foster use of electronic media by providers; automated tools which do not yet provide for extracting information; and highly reliable OCR, according to Dennis Clift, chief of staff, Defense Intelligence Agency (DIA).

Multimedia Challenges

Multimedia is coming and with it a different series of problems, both

technological and managerial. Multimedia presents an order of magnitude with tens of terabytes more than text, explained William Ruh, the MITRE Corp.

Integration and scale-up are not trivial. The system breaks down when larger volume is introduced. The user will have orders of magnitude, more information to assimilate and even if there is perfect retrieval, the user will get too much to read. The user should have tools to assimilate—that is the challenge of a current MITRE project.

Each source has a different method of access, e.g., communication protocols and query languages. There are additional legalities of usage involving copyright and cost, and an increasing risk of unautho-

rized disclosure. We need to think how put multimedia online and how to manage it. Also needed is more understanding the information itself for better indexing.

Technology is not consistently mature. OCR and machine translation require continued investment. And, Ruh adds information organization, a tough issue deal with, is the issue.

Information Warfare and Terrorism

Computer warfare can destroy competitors by destroying an organization's information infrastructure. Malicious software, communication interception public-switched networks, electromagnetic eavesdropping, use of HERF (high energy radio frequency) and HERO (high energy radiation ordnance) are some of the new weapons. Many techniques are invisible and can be used remotely, explained William Schwartz, Information Warfare. We don't know the extent which these events are occurring.

War on Drugs

Intelligence can be trained for use the war on drugs. A multimedia collection of tools and methods with multidisciplinary team of librarians, scientists, policy people, and number crunchers is being developed at Los Alamos. The approach, said Dr. James Holden-Rhodes, ensures depth, breadth, and balance providing models and simulations of drug trafficking sources, transfers, organizations, and family linkages.

CENDI

Outside the intelligence community semi-official group brings together senior STI advisers and serves as a model interagency cooperation on OS issues. The group, CENDI, consists of representatives from Commerce, Energy, NASA, National Library of Medicine, and Department of Defense. Issues CENDI is grappling with are duplication of effort, overlapping sources, gaps, competition with the information industry; information analysis; quality; and standards. Work level issues include formats, transfer protocols, and specific content of STI, said Kurt Moholm, chairman.

Restructuring Intelligence

DOD has "one million workstations hobbled together in little networks," the cost of supporting these workstations is horrendous, said Paul Strassman, Director of DOD information. The mass effort to streamline information assets to a secure, highly distributed system includes systems integration, some 1,700 data processing sites, and about 20,000 personnel. One example of current redundancy: synonyms for the word "unit."

Strassman advised: Don't bring in new technology to make the system worse. First, streamline and simplify; then consider the machine.

The greatest lack in intelligence today, according to Steele, is the way that the intelligence community is structured. It is biased toward classification and not to access of information at relatively low cost. OS should be the first resort, he said, which is not the case now. The great

(continued on next page)

MICROCOMPUTER INDEX

Lisa Jasper and Bill Spence, Editors

Microcomputer Index is a quarterly abstracts journal covering the most important and widely read microcomputer publications, including: mass-market and wide-circulation magazines; publications focusing on specific installed hardware/software bases and business aspects of microcomputing; and journals dealing with educational and library use of microcomputers. Over 170 publications have been included in *Microcomputer Index* since its inception in 1981, and more than 75 are currently abstracted. Each year *Microcomputer Index* publishes over 12,000 abstracts and citations to the literature related to personal computer software, hardware, networks, databases, communications, books, industry events, corporate information, and more.

Abstracts are divided into seven categories, and within each category abstracts are listed alphabetically by primary subject. Categories include: Articles, News, and Columns; Book Reviews; Buyers and Vendor Guides; Hardware Reviews; Product Announcements; Program Listings; and Software Reviews. In addition, there are five indexes—Author, Company Name, Product Name, Compatible Hardware and Software, and Subject—which provide access to the literature.

The Company Name Index provides citations to articles on the activities of some 4,000 companies and organizations within the microcomputer industry. More than 6,000 product names (hardware, software, books, etc.) are included in the Product Name Index. The Compatible Hardware and Software Index is an index to the microcomputer systems with which a particular software package is compatible and also indicates any other packages or programs needed to run a particular type of software. The Subject Index is an index to all descriptions associated with each abstract. The Author Index provides an alphabetical listing of each author.

Subscriptions also include an annual Cumulated Index, which is published separately at the end of each volume year.

Volume 14 (1993)/4 issues a year/ISSN: 8756-7040
1 year \$165.00/Canada & Mexico \$171.00 (U.S. funds)

Express Order Service: 609-654-6266

Fax Order Service: 609-654-4309

Mail Orders: Complete and mail the form below to:

Learned Information, Inc., 143 Old Marlton Pike, Medford, NJ 08055

☐ YES! Please enter my 1 year subscription to *Microcomputer Index* at \$ _____

Name _____

Title _____

Organization _____

Department _____

Address _____

City/State/Zip _____

Daytime Phone _____

Method of Payment: ☐ Payment enclosed

☐ Invoice me Purchase Order # _____

I prefer ☐ MasterCard ☐ Visa Account # _____

Exp. Date _____ Signature _____

MICROCOMPUTER INDEX

1993

An Abstracts Journal
Covering 2,879 Magazine Articles
& News Items Including
1,236 Reviews of Software
Hardware & Books

U. S. Intelligence

(continued from previous page)

asset of intelligence is the analysis methodology for fusion of image, signals, and human intellect.

There's a need for modern information technology tools. Technology is far advanced of where the CIA is now and a process is needed for change in the intelligence community, said Howard Rheingold, editor of the *Whole Earth Review* and author of several books on virtual reality.

Steele agrees and calls for user interface changes with elegant, intuitive CAI-embedded interfaces. Steele also thinks that the information industry is too proprietary. Asked how companies will stay in business if not proprietary, he replied that "they retain their market share by building a better system; integrate new technologies and new techniques; and do it better than any one else."

Visions of the Future

Planning any restructuring of intelli-

gence, whether government or private sector, should recognize three driving forces, Kahn advised:

- Network growth—the community; the size of networks; the amount of traffic;
- Higher speeds and technology: gigabits; all optical networks; advanced workstations and supercomputers;
- Grass roots: K-12; small business; libraries; state and local governments.

Coming changes include moving to an image-based networking environment; undulating workstations or LANs with an abundance of input from which to collect; linking high performance computers at gigabit speeds; integrating remote sources of high-speed data and large databases; and time compression.

The motivation for these changes, Kahn said, are economics, competitive requirements, and that innovations are big enablers for science, medicine, business, national security, finance, government, and education.

Steele's vision of intelligence in the year 2000? Eighty percent of what is done now will be found in personalized newspapers and alerts. The intelligence community will go back to basics: Their unique clandestine and technical information. And OS will truly be the first resort for intelligence and for other users.

Putting Your Money Where Your Interest Is

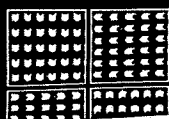
The planners were surprised by the

number of people that attended the symposium. About 200 were expected, over 600 were there. Three cultures were represented: intelligence and two sectors of the information community—the conventional players and the hackers. Steele defined a hacker as a computer programmer who writes a brilliant, elegant piece of work as contrasted with a cracker who does the break-ins.

Many table top exhibits gave participants the opportunity for hands-on experience with OS information, and ideas abounded for the second International Symposium.

Lois F. Lunin is an information consultant, editor, and writer based in Washington, D.C.

ANNUAL REVIEW OF
INFORMATION
SCIENCE AND
TECHNOLOGY



ANNUAL REVIEW OF
INFORMATION
SCIENCE AND